CLAIMS

1. A method for transmitting data between a GRPS/EDGE radio access network GERAN and user equipment of a mobile system, comprising the steps of:

encrypting the data to be transmitted using an encryption algorithm at the transmitting end,

transmitting the encrypted data from the transmitting end to the receiving end,

decrypting the transmitted data using an encryption algorithm at the receiving end,

wherein an encryption algorithm of the radio access network UTRAN employing the wideband code division multiple access method of the universal mobile telecommunications system is used as the encryption algorithm, in which case the input parameters of agreed format required by the encryption algorithm are created on the basis of the operating parameters of the GPRS/EDGE radio access network GERAN.

2. A method as claimed in claim 1, wherein the agreed format of the input parameters of the encryption algorithm defines the number of the input parameters and the length of each parameter.

3. A method as claimed in claim 1, wherein the encryption algorithm is a black box and its implementation exactly the same in both the GPRS/EDGE radio access network GERAN and the radio access network UTRAN employing the wideband code division multiple access method.

4. A method as claimed in claim 1, wherein the input parameters comprise a counter parameter.

5. A method as claimed in claim 4, wherein the counter parameter comprises a symbol which defines whether the data to be encrypted is data of the second layer signaling plane or other data.

6. A method as claimed in claim 1, wherein the input parameters comprise a bearer parameter, and one of the bearer parameter values is reserved for signaling plane data to be encrypted.

7. A method as claimed in claim 4, wherein when executing the encryption algorithm in the MAC layer of a protocol stack, the counter parameter comprises an extended TDMA frame number.

8. A method as claimed in claim 7, wherein the extended TDMA frame number is based on extending the T1 counter part of GSM.

9. A method as claimed in claim 7, wherein information on the last used extended TDMA frame number is stored in the user equipment for the next connection.

10. A method as claimed in claim 9, wherein the information to be stored on the last used extended TDMA frame number comprises a certain number of the most significant bits of the extended TDMA frame number, and before the information is used in a new radio connection to form an extended TDMA frame number, the value of the number formed by said most significant bits is increased by one.

11. A method as claimed in claim 4, wherein when executing the encryption algorithm in the MAC layer of a protocol stack, the counter parameter comprises a time slot number.

12. A method as claimed in claim 4, wherein when executing the encryption algorithm in the RLC layer of a protocol stack, the counter parameter comprises a hyper frame number.

13. A method as claimed in claim 12, wherein information is stored on the last used hyper frame number in the user equipment for the next connection, and before the information is used in a new radio connection to form a hyper frame number, the value of the number formed by said most significant bits is increased by one.

14. A method as claimed in claim 13, wherein the information to be stored on the last used hyper frame number comprises a certain number of the most significant bits of the hyper frame number.

15. A method as claimed in claim 1, wherein when the connection of the user equipment changes between the GPRS/EDGE radio access network GERAN and the radio access network UTRAN employing wideband code division multiple access method, information on the last used extended TDMA frame number or hyper frame number is provided to the new radio access network, and the same encryption key input parameter as in the old radio access network is used as the encryption key input parameter of the encryption algorithm in the new radio access network.

16. A method as claimed in claim 15, wherein the information to be provided comprises a certain number of most significant bits, and before the

information is used in a new radio access network, the value of the number formed by said most significant bits is increased by one.

17. User equipment of a mobile system, comprising

means for encrypting data to be transmitted to a GPRS/EDGE radio access network GERAN using an encryption algorithm,

means for decrypting data received from the GPRS/EDGE radio access network GERAN using an encryption algorithm;

wherein the encryption algorithm is an encryption algorithm of the radio access network UTRAN employing the wideband code division multiple access method of the universal mobile telecommunications system, and the user equipment comprises means for creating the input parameters of agreed format required by the encryption algorithm on the basis of the operating parameters of the GPRS/EDGE radio access network GERAN.

18. User equipment as claimed in claim 17, wherein the agreed format of the input parameters of the encryption algorithm defines the number of the input parameters and the length of each parameter.

19. User equipment as claimed in claim 17, wherein the encryption algorithm is a black box and its implementation exactly the same in both the GPRS/EDGE radio access network GERAN and the radio access network UTRAN employing the wideband code division multiple access method.

20. User equipment as claimed in claim 17, wherein the input parameters comprise a counter parameter.

21. User equipment as claimed in claim 20, wherein the counter parameter comprises a symbol which defines whether the data to be encrypted is data of the second layer signaling plane or other data.

22. User equipment as claimed in claim 17, wherein the input parameters comprise a bearer parameter, and one of the bearer parameter values is reserved for signaling plane data to be encrypted.

23. User equipment as claimed in claim 20, wherein when executing the encryption algorithm in the MAC layer of a protocol stack, the counter parameter comprises an extended TDMA frame number.

24. User equipment as claimed in claim 23, wherein the extended TDMA frame number is based on extending the T1 counter part of GSM.

25. User equipment as claimed in claim 23, wherein the user equipment comprises means for storing information on the last used extended TDMA frame number for the next connection.

26. User equipment as claimed in claim 25, wherein the information to be stored on the last used extended TDMA frame number comprises a certain number of the most significant bits of the extended TDMA frame number, and the user equipment comprises means for increasing by one the value of the number formed by said most significant bits before the information is used in a new radio connection to form an extended TDMA frame number.

27. User equipment as claimed in claim 20, wherein when executing the encryption algorithm in the MAC layer of a protocol stack, the counter parameter comprises a time slot number.

28. User equipment as claimed in claim 20, wherein when executing the encryption algorithm in the RLC layer of a protocol stack, the counter parameter comprises a hyper frame number.

29. User equipment as claimed in claim 28, wherein the user equipment comprises means for storing information on the last used hyper frame number for the next connection.

30. User equipment as claimed in claim 29, wherein the information to be stored on the last used hyper frame number comprises a certain number of the most significant bits of the hyper frame number, and the user equipment comprises means for increasing by one the value of the number formed by said most significant bits before the information is used in a new radio connection to form a hyper frame number.

31. User equipment as claimed in claim 17, wherein the user equipment comprises means for providing information on the last used extended TDMA frame number or hyper frame number to the new radio access network when the connection of the user equipment changes between the GPRS/EDGE radio access network GERAN and the radio access network UTRAN employing wideband code division multiple access method, and for using the same encryption key parameter as in the old radio access network as the encryption key parameter of the encryption algorithm in the new radio access network.

32. User equipment as claimed in claim 31, wherein the information to be provided comprises a certain number of most significant bits, and the user equipment comprises means for increasing by one the value of the number formed by said most significant bits before the information is used in a new radio access network.

33. A GPRS/EDGE radio access network GERAN of a mobile system, comprising

means for encrypting data to be transmitted to user equipment using an encryption algorithm,

means for decrypting data received from the user equipment using the encryption algorithm;

wherein the encryption algorithm is an encryption algorithm of the radio access network UTRAN employing the wideband code division multiple access method of the universal mobile telecommunications system, and the GPRS/EDGE radio access network GERAN comprises means for creating the input parameters of agreed format required by the encryption algorithm on the basis of the operating parameters of the GPRS/EDGE radio access network GERAN.

34. A GPRS/EDGE radio access network as claimed in claim 33, wherein the agreed format of the input parameters of the encryption algorithm defines the number of the input parameters and the length of each parameter.

35. A GPRS/EDGE radio access network as claimed in claim 33, wherein the encryption algorithm is a black box and its implementation exactly the same in both the GPRS/EDGE radio access network GERAN and the radio access network UTRAN employing the wideband code division multiple access method.

36. A GPRS/EDGE radio access network as claimed in claim 33, wherein the input parameters comprise a counter parameter.

37. A GPRS/EDGE radio access network as claimed in claim 36, wherein the counter parameter comprises a symbol which defines whether the data to be encrypted is data of the second layer signaling plane or other data.

38. A GPRS/EDGE radio access network as claimed in claim 37, wherein the input parameters comprise a bearer parameter, and one of the bearer parameter values is reserved for signaling plane data to be encrypted.

39. A GPRS/EDGE radio access network as claimed in claim 36, wherein when executing the encryption algorithm in the MAC layer of a protocol stack, the counter parameter comprises an extended TDMA frame number.

40. A GPRS/EDGE radio access network as claimed in claim 39, wherein the extended TDMA frame number is based on extending the T1 counter part of GSM.

41. A GPRS/EDGE radio access network as claimed in claim 39, wherein the GPRS/EDGE radio access network GERAN comprises means for storing information on the last used extended TDMA frame number for the next connection.

42. A GPRS/EDGE radio access network as claimed in claim 41, wherein the information to be stored on the last used extended TDMA frame number comprises a certain number of the most significant bits of the extended TDMA frame number, and the GPRS/EDGE radio access network GERAN comprises means for increasing by one the value of the number formed by said most significant bits before the information is used to form an extended TDMA frame number.

43. A GPRS/EDGE radio access network as claimed in claim 36, wherein when executing the encryption algorithm in the MAC layer of a protocol stack, the counter parameter comprises a time slot number.

44. A GPRS/EDGE radio access network as claimed in claim 36, wherein when executing the encryption algorithm in the RLC layer of a protocol stack, the counter parameter comprises a hyper frame number.

45. A GPRS/EDGE radio access network as claimed in claim 44, wherein the GPRS/EDGE radio access network GERAN comprises means for storing information on the last used hyper frame number for the next connection.

46. A GPRS/EDGE radio access network as claimed in claim 45, wherein the information to be stored on the last used hyper frame number comprises a certain number of the most significant bits of the hyper frame number, and the GPRS/EDGE radio access network GERAN comprises means for increasing by one the value of the number formed by said most significant bits before the information is used to form a hyper frame number.

47. A GPRS/EDGE radio access network as claimed in claim 33, wherein the GPRS/EDGE radio access network GERAN comprises means for receiving information on the last used extended TDMA frame number or hyper frame number to the user equipment when the connection of the user equipment changes between the GPRS/EDGE radio access network GERAN and the radio access network UTRAN employing wideband code division multiple access method, and for using as the encryption key parameter of the encryption algorithm, the encryption key parameter according to the received information.

48. A GPRS/EDGE radio access network as claimed in claim 47, wherein the information to be provided comprises a certain number of most significant bits, and the GPRS/EDGE radio access network GERAN comprises means for increasing by one the value of the number formed by said most significant bits before the information is used.